IN THE CLAIMS:

1. (cancelled) A method for verifying the identity of a message-originator program (D) by a message-receiver program comprising the steps of receiving from said message-originator program (D) a message comprising a program-specific identifier (H(D)), which has been provided for said message-originator program (D) by means of a trusted computing base (TCB), and verifying whether said received program-specific identifier (H(D)) is known to said message-receiver program.

2. (currently amended) A method for disclosing the identity of a message-originator program (D) to a message-receiver program (S), the method comprising:

sending from said message-originator program (D) to said message receiver program (S) a message comprising a program-specific identifier (H(D)), which has been provided for said message-originator program (D) by means of an automatic operation of applying a hash function (H) to said message originator program in a trusted computing base (TCB) in which said trusted computing base applies said hash function to said message originator program in response to a request from said message originator program, the result of which hash function is said program-specific identifier, said program-specific identifier (H(D)) being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S).

3. (currently amended) A method for verifying the identity of a message-originator program (D) by message-receiver program (S), the method comprising the steps of:

providing a program-specific identifier (H(D)) for said message-originator program (D) by means of an automatic operation of applying a hash function (H) to said message originator program in a trusted computing base (TCB), in which said trusted computing base applies said hash function to said message originator program in response to a request from said message originator program, the result of which hash function is said program-specific identifier;

sending from said message-originator program (D) to said message-receiver program (S) a message comprising said program-specific identifier (H(D)),

receiving at said message-receiving program (S) said message; and

verifying whether said received program-specific identifier (H(D)) is known to said message-receiver program (S).

4. (Currently amended) Method according to claim ~~1~~ 3, wherein the message-receiver program afterwards becomes a response message-originator program and sends a response message to the message-originator program comprising:

a response-program-specific identifier (H(S)), which has been provided for said response-message originator program by means of the trusted computing base (TCB); and

an acknowledgment of the program-specific identifier (H(D)) has been verified as being known.

5. (cancelled) Method according to claim 1, wherein a substantially unique cryptographic identifier that is derived by applying a cryptographic function (H) to the message-originator program (D), preferably a hash function, and more preferably a one-way hash function, such as MD5 or SHA-1, is used as the program-specific identifier (H(D)).

6. (cancelled) Method according to claim 1, further comprising the step of signing the program-specific identifier (H(D)) and/or the message by use of a private cryptographic key (k^{-1}) to establish trust between different programs.

7. (currently amended) Method according to claim ~~1~~ 3, wherein the message further comprises an additional program-specific identifier (H(G)) that is signed by use of ~~the~~ a private cryptographic key (k^{-1}) acceptable to said message receiver program to establish a membership of an additional program in a trust relationship, in which said private cryptographic key is supplied by a helper program that is known to said message-receiver program and knows said message originator program; and

said helper program receives an additional private key and an additional program specific identifier from said additional program;

said helper program verifies that said additional program is known to it; and

said helper program sends said additional private key and additional program specific identifier to said message receiver program;

said message receiver program adds said additional private key and additional program specific identifier to a stored list of known program specific identifiers, whereby said additional program is added to said trust relationship.

8. (cancelled) Method according to claim 1, wherein the message receiver-program (S) has a public cryptographic key (k).

9. (cancelled) Method according to claim 1, wherein the message-receiver program (S) and/or the trusted computing base (TCB) uses(s) a list comprising pre-stored program-specific identifiers and wherein said message-receiver program (S) verifies whether the program-specific identifier (H(D)) is identical to one of said pre-stored program-specific identifiers.

10. (cancelled) Method according to claim 1, wherein the message-receiver program (S) sends a rejection-message if the program-specific identifier (H(D)) is not verified as being known.

11. (Currently amended) Method according to claim ~~1~~ 3, wherein the message-originator program (D) and the message-receiver program (S) are executed on different systems and are connectable via a network, each having its trusted computing base (TCB) for providing program-specific cryptographic identifiers.

12. (currently amended) A computer program comprising program code means for performing the steps of claim ~~1~~ 3, when said program is run on a computer.

13. (currently amended) A computer program product comprising program code means stored on a computer readable medium for performing the method of claim ~~1~~ 3, when said program product is run on a computer.

14. (currently amended) An apparatus for verifying the identity of a message-originator program (D) by a message-receiver program (S) on a computer, the apparatus comprising:

computing means;

a receive module for receiving from said message-originator program (D) a message comprising a program-specific identifier (H(D)), which has been provided for said message-originator program (D) by means of a trusted computing base (TCB), and

a verifier-module that verifies whether said program-specific identifier (H(D)) is known to said message-receiver program (S).

15. (cancelled) An apparatus for disclosing the identity of a message-originator program (S) on a computer, the apparatus comprising:

computing means;

a trusted computing base (TCB) comprising a generator-module for creating a program-specific identifier (H(D)), and

a sender-module for sending from said message-originator program (D) a message comprising said program-specific identifier (H(D)), said program-specific identifier (H(D)) being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S).

16. (newly added) A method according to claim 7, in which said helper program is invoked after said message originator program has been rejected by said message receiver program.

17. (newly added) A method according to claim 7, in which said helper program is invoked to perform a computation function.

18 (newly added) A method according to claim 16, in which said helper program is invoked said message originator program without human intervention.

19 (newly added) A method according to claim 17, in which said helper program is invoked said message originator program without human intervention.